MINUTES OF THE JANUARY 15, 2014, MEETING OF THE DATA SECURITY AND PRIVACY COMMITTEE HEALTH INFORMATION EXCHANGE AUTHORITY

The Data Security and Privacy Committee ("DSPC") of the Illinois Health Information Exchange Authority ("Authority"), pursuant to notice duly given, held a meeting of the 9:00 AM on January 15, 2014, at the State of Illinois Thompson Center, 100 W. Randolph, Room 9-031, Chicago, Illinois 60601, with telephone connectivity.

Appointed Committee Members Present:	**Staff Present:**
Dr. Nicholas Panomitros	**Raul Recarey**
Jay Anderson	**Krysta Heaney**
Elissa Bassler	**Elizabeth LaRocca**
Jud DeLoss [phone]	**Kerri McBride**
Dr. Carl Gunter [phone]	
Debbie Hayes [phone]	
David Holland [phone]	
Tiefu Shen [phone]	
Mick Skott [phone]	
William Spence [phone]	

Welcome and Call to Order

Dr. Nicholas Panomitros, Chairman of the Data Security and Privacy Committee, called the meeting to order.

Roll Call

Ms. Elizabeth LaRoccca, Office of Health Information Technology (OHIT) General Counsel and Assistant Secretary to the Board, confirmed the presence of the Members of the Data Security and Privacy Committee indicated above.

Review and Discussion of Draft Privacy Policies

Dr. Nicholas Panomitros, Chairman of the Data Security and Privacy committee, began the discussion by providing background information on the draft Privacy Policies developed by the staff. He explained that the policies were developed following a review of other state and regional HIE's policies and procedures, Illinois law, and federal law, including HIPAA and HITECH. The purpose of these policies is to lay a foundation for ILHIE operations by ensuring the privacy and security of health data transmitted through the ILHIE.

Discussion of ILHIE Privacy and Security Governance

The discussion began with ILHIE Privacy and Security Governance Policy. Beth LaRocca explained that these policies are meant to give guidance in ILHIE operations and put into written form some

procedures already in place. These policies largely codify what is already law in the form of the enabling statute of the ILHIE authority. This also includes how policies and procedures will be reviewed up to the board level. Kerri McBride clarified that Data Security and Privacy Committee is not redefining HIPAA terms.

Dr. Carl Gunter wanted clarification that this committee is an oversight committee and will continue to exist as long as ILHIE exists. He commented that there is nothing about turnover/tenure of committee members. Beth clarified that this information is in the by-laws and a board resolution. Beth said she can send the information out. Dr. Gunter suggested a sentence or two that spells out the tenure for committee members.

Question: Will ILHIE have the authority to terminate a user for noncompliance using more narrow restrictions?
Answer: Each contract has slightly more specific requirements, like having to have their own privacy and security policies – mostly policies required by HIPAA. If there is a breach, ILHIE will make sure they mitigate the breach but if they continue to have the same person in the same position and they continue to breach, then they will suspend that party's access.

A committee member suggested a clarification that some of the language ILHIE is using is not a direct quote from the law.

Discussion of Compliance with Law and Policy

This policy says that all participants shall comply with applicable law and ILHIE policies and procedures. Applicable law is Illinois and federal (HIPAA, HITECH).

The committee clarified information regarding the e-Health exchange policy. The e-Health exchange is a national network for exchanging health information. It will be the ILHIE's method of exchanging data with other states. One limitation is that it has a slightly more limited purpose – it only allows research if you have a specific consent from the individual. ILHIE will be using it when it exchanges data with the Veterans Administration and Social Security Administration. A committee member suggested adding the term "e-Health exchange" to the definitions list.

Question: How would policy number 1.1 be enforced?
Answer: The participants, if they are working in the health care field, will have to be compliant with laws and policies. If ILHIE's laws and policies change, we can put a notice on the website. A committee member commented that this policy seems unenforceable. Another member suggested maintaining a mailing list to inform people of changes that are relevant to the system. Using this mechanism, you could enforce compliance following notification.

Question: For policy 2.2, what is the process for determining whose policy better protects an individual's health information?
Answer: It goes back to the participant to determine the best way to protect PHI. The policy is not trying to substitute the Authority as the enforcer of HIPAA and HITECH, for example. The Authority isn't substituting its judgment for the provider. The participants must meet the Authority's policies. If a provider has a policy that is stricter, the Authority will generally accept it as long as it's reasonable and logical.

A committee member suggested including a clause that might allow the Authority and the participant to explore compliance status together. Currently, there is no stipulation that these providers would cooperate with a review of their compliance. The Authority doesn't want to make final determinations because it doesn't want to be brought under the APA. The prime enforcement mechanism for compliance is the contract. The committee suggested being careful not to scare away participants because of certain enforcement models and must balance this with public trust of the ILHIE. While there is already language that says the Authority can monitor compliance, staff agreed to review the wording to possibly add language regarding participant cooperation.

Question: Who decides what best protects EHR information?
Answer: It's subjective, but ILHIE must decide if it is the participant or ILHIE. The committee said that if there is a conflict, it will likely be up to the ILHIE to decide what best protects EHR information.

A committee member suggested spelling out certain acronyms and/or link to HIPAA for certain terms for reference of which terms are in the definitions. HIPAA definitions were incorporated, but the committee agreed to try to make it more clearly articulated.

Question: When we say "apply with all applicable laws," can this be limited to HIPAA requirements?
Answer: With regards to PHI, HIPAA doesn't cover items that are protected by Illinois law or other federal law.

The committee discussed at length "all applicable law." There was a concern that the language might be too broad, but limiting "all applicable law" to just HIPAA and HITECH might send the wrong message to patients. HIPAA and HITECH don't cover information like substance abuse and mental health treatment information and patients might not be comfortable sharing that information if it isn't protected. At a minimum, each organization or provider would be expected to comply with laws that are applicable to the exchange of health information data through the Exchange.

Question: The language says "you will comply with these policies and procedures" and then "to the extent required by applicable law." Why not say "you will comply with these policies and procedures?"
Answer: Applicable law covers the possibility that information will go to or come from a different state.

Someone then commented that "to the extent" could be read to mean full compliance isn't required.

Discussion of Privacy Policy #1 – User Authentication

Beth gave an overview of the policy. She said this is meant to speak to the participant about how they need to ensure that their authorized users are who they say they are, what technical standards apply, having a unique identifier and password, re-authentication policies.

Question: How does the ILHIE authority designate an authorized user within a participant organization? Why not just participants?
Answer: ILHIE authority will have its own authorized users. The committee is now considering using the term "respective organizations."

Question: The policies require using the identification and authentication procedures in accordance with NIST level 3 guidelines, but later it lists the components of the authentication and identification procedures. Are the NIST guidelines not enough?
Answer: These are two different concepts. One involves a high-level person providing an affidavit, for example an individual organization's administrator has to be authenticated by providing different forms of identification (like a bank account). NIST Level 3 is a high level multi-factor authentication like what a bank would use. ILHIE is mandated to implement NIST level 3 guidelines with the direct exchange, so the committee is trying to carry over these guidelines with the exchange. Directtrust.org mandates that we use NSIT Level 3 authentication.

The committee then discussed security guidelines with respect to the NIST guidelines. The committee agreed that security and the strongest privacy protections were the most important consideration. The committee agreed to look at this language to make sure it was consistent with current security obligations.

Question: Does ILHIE want to have a role in governing password strength, time-out times, and similar security measures?
Answer: ILHIE isn't dictating those requirements, just that each organization has those requirements in place. Dr. Gunter found a national HIE governance forum document from Dec. 2013 that gives detailed guidance on levels of assurance for authentication.

A member commented that the overall top-level description of the policy should be "for implementing NIST level 3 and other…" because NIST does not cover log-ins and passwords.

Discussion of Privacy Policy #2 – User Authorization

A member commented that if the definition of "subcontractor" is the definition provided under HIPAA, he doesn't want to impose a training obligation on the participant or the subcontractor. Another member clarified that if the subcontractor is going to be an authorized user for a covered entity who is a participant and the participant is vouching for that sub in letting them have access, then the participant must be responsible for being training on accessing. The committee agreed to re-review this policy and how people are identified throughout. Another member expressed concern that small providers may find this requirement worrisome because they don't have an established training program and might expect the party they hire in having more expertise. A member suggested that the language could be revised to reflect that the participant can delegate the security and awareness training program to a sub-contractor or assure that the sub-contractor will do it.

In section 2.3, it says that access to ILHIE is immediately revoked for material breach of policies and procedures but in 3.0 it "may" be suspended. A member clarified that 2.3 is specific about a breach of data sharing and policies and procedures or other non-compliance but 3.0 specifically about a Breach under HIPAA.

Question: Is the ILHIE going to maintain the authorizations?
Answer: It isn't practical for ILHIE to be responsible for all the authorizations. The participants will manage a list of parties who have authorization through them. The management of list of authorized users cannot be done by ILHIE alone. A member clarified that the system administrator has access – in the contract, there is a list of requirements for what a system administrator must do.

A member wanted clarification on how the authorization process will work if someone wants to access a similar system. Another member clarified that unless you're using direct, you won't be able to specify the hospital you want to contact. In a bidirectional system, ILHIE would collect health information from every provider that has treated a person and send it back to the requesting provider.

The committee discussed adding user access. Access is provider specific, each organization determines how access is delegated. Access could be automated. You would need approval from administrator and if you have that approval, access could be granted quickly. Some hospitals might pre-approve all doctors and then allow them access as needed instead.

Discussion of Privacy Policy #3 – Access, Use and Disclosure of Protected Health Information

This policy discusses when PHI can be requested or disclosed by a participant and how ILHIE may access or transmit information

A member commented that in 2.4i, the concept of ILHIE being able to collect and aggregate for public health reporting, MU and medical research is beyond the scope of what ILHIE was designed for. The committee agreed to review this language and keep the language open to amendment in the future. There should be a pathway for review for research in the future while making sure people understand what research means. At this point, any sort of written research would need written authorization from a patient. Our exchange is set up as a clinical exchange for clinical purposes. The committee agreed to change the language and keep it open for developing whatever extensions of ILHIE would be approved for research.

Discussion of Privacy Policy #4 – Patient Choice and Meaningful Disclosure

This policy has already been reviewed and approved by the board

Discussion of Privacy Policy #5 – Information Subject to Special Protection

This policy requires that each participant must have the appropriate permissions to share specially protection health information.

A member asked if section 1.3 was the proper place for the out-of-pocket exclusion. The committee is open to suggestions regarding location. This is information that providers are required to prevent the disclosure of information they must block if the individual patient wants blocked.

Discussion of Privacy Policy #6 – Emergency Access

This policy did not need to be reviewed.

Discussion of Privacy Policy #7 – Individual Access to Data, Discussion of Privacy Policy, #8 – Individual Amendment of Data, Discussion of Privacy Policy #9 – Individual Accounting of Disclosures

ILHIE does not keep a designated record set, ILHIE can't provide access nor can ILHIE can do an amendment of data. ILHIE can assist the participants that are covered entities in #7, 8 and 9, with regard to accounting and can provide an accounting of who has accessed data through the ILHIE.

Discussion of Privacy Policy #10 – Minimum Necessary

No comments.

Discussion of Privacy Policy #11 – ILHIE Workforce, Agents, Contractors and Subcontractors

This is related to the same discussion regarding authorized purposes in policy 3, section 2.4. This will be made consistent with 2.4 of policy 3.

Discussion of Privacy Policy #12 – Complaint Handling and Resolution

This policy sets out a process by which the ILHIE Authority can accept complaints by anyone who has taken an issue with something that the ILHIE or one of its participants is doing. It sets out how ILHIE will accept those complaints and work to resolve them.

Question: With respect to the investigation, how are we addressing maintaining privilege with the cooperation clause and attorney-client privilege?
Answer: This is similar to provisions discussed in the breach work group. One of the non-final policies said the participant had no obligation to turn something over that was protected by privilege, but there was then a consensus to remove that language because the committee assumined no privileged documents will be turned over. ILHIE is expecting that counsel would raise privilege when discussing an issue. The committee agreed to look at the final breach language and transfer it to this policy.

Question: Is any of this subject to open records and FOIA?
Answer: The committee will have to look at the language again. There are some strict limitations on what is subject to FOIA.

Discussion of Privacy Policy #13 – Sanctions

A member commented that there is a lot of cross-over with policy #2 and this policy. This policy will be re-worked to be consistent with #2.

Question: Would this allow one participant to blacklist another?
Answer: One participant could block another from reading their information and that is something ILHIE can't do at this point. The individual cannot limit who sees their information. A member suggested that it might be better for participants to express their concerns about others and have the exchange decide on the limitation rather than running the risk that the participants try to block each other.

Discussion of Privacy Policy #14 – Enforcement

A member commented that there is no need to talk about random audits; at any point in time you can collect audit records you need for an investigation. For further clarification, the point of a random is that we can do it at any time, but the committee agreed the language would need to be changed to specify that the ILHIE can do audits at any point in time.

Question: Will the participants have the ability to run their own audits?

Answer: ILHIE would be able to run a query for them. The currently audit policy is that there are requirements that the participant has its own audit procedures. If ILHIE ask a participant for an audit log, the participant would generate it from the participant's records.

A member commented that the language surrounding audit logs should be more vague and give more discretion to the people who collect the audit logs. The language should be less specific or more keyed to a summary of the information.

Next Steps:

The group agreed that two more meetings were necessary. The group needs to have a recommendation to be presented to the Board on April 2. The group agreed to have another meeting in February and another meeting in March.

Public Comment:

One public commented asked to see a demo of the system. The committee agreed that a demo system might be able to be set up.

Adjournment:

There was no quorum and the committee didn't need a movement to adjourn.

Minutes submitted on 2/10/14 by Sarah Nichelson